

Стеганоанализ алгоритма Коха-Жао

С.В. Белим
sbelim@mail.ru

Д.Э. Вильховский
vilkhovskiy@gmail.com

Омский государственный университет им. Ф.М. Достоевского, Омск, Россия

Аннотация

Проведен анализ стеганографического алгоритма Коха-Жао. Рассмотрена возможность атаки на обнаружение сообщения. Предложен алгоритм вычисления границ встроенного сообщения, основанный на анализе коэффициентов дискретного косинусного преобразования. Проведен компьютерный эксперимент. Определены параметры встраивания, позволяющие осуществить атаку.

Введение

Основной целью стеганографического анализа (стеганоанализа) является исследование стойкости схемы стеганографического встраивания к атакам различного типа. Традиционно формулируется три основные задачи стеганоанализа. Первая задача состоит в обнаружении факта наличия встроенного сообщения. При обнаружении встроенного сообщения ставится задача вычисления его размера и расположения в контейнере. Третьей и самой сложной задачей является извлечение встроенного сообщения и его интерпретация без каких-либо данных о параметрах встраивания.

На сегодняшний день основные успехи стеганоанализа связаны с решением первой задачи. Причем применяются преимущественно статистические методы исследования контейнера с встроенным сообщением. Все эти методы основаны на предположении о том, что встраивание сообщения вносит изменения в статистические характеристики контейнера, которые могут быть обнаружены на основе исследования различных распределений. Так в статьях [4, 5] делают предположение о случайном характере распределения младших битов синей компоненты и на его основе применяют критерий χ -квадрат для задачи обнаружения стегановставки. Предложенный метод дает хорошие результаты при равномерном заполнении контейнера. Для решения второй и третьей задачи статистических методов недостаточно и необходимо применять интеллектуальные алгоритмы. Например в статьях [6, 7, 8, 9] для анализа младшего слоя используется метод анализа иерархий, что позволяет с высокой степенью точности определить размеры и положение встроенной информации.

Целью данной работы является стеганоанализ алгоритма Коха-Жао [10].

1 Алгоритм встраивания и постановка задачи

В качестве исходного объекта будем рассматривать изображение, в которое предположительно осуществлено встраивание сообщения. Достоверная информация о том было осуществлено встраивание или нет отсутствует. Однако известно, что встраивание могло быть осуществлено только методом Коха-Жао [10]. Причем встраивание сообщения могло быть осуществлено только непрерывным блоком. Поставим задачу обнаружения факта встраивания и извлечения встроенного сообщения, если оно присутствует.

Copyright © by the paper's authors. Copying permitted for private and academic purposes.

In: Sergey V. Belim, Nadezda F. Bogachenko (eds.): Proceedings of the Workshop on Data, Modeling and Security 2018 (DMS-2018), Omsk, Russia, October 2018, published at <http://ceur-ws.org>

Метод стеганографического встраивания Коха-Жао [10] использует двумерное дискретное косинусное преобразование и может быть записано в виде следующего алгоритма:

1. Разбить исходное изображение на блоки размером 8×8 пикселей.
2. Применить дискретное косинусное преобразование к каждому блоку. Получить набор матриц коэффициентов D_i ($i = 1, \dots, N$; N – количество блоков) размером 8×8 .
3. Выбрать блоки для встраивания. Записать в каждый выбранный блок 1 бит встраиваемой информации.
4. В каждом блоке выбрать два коэффициента дискретного косинусного преобразования ДКП в каждом блоке симметричные относительно главной диагонали. Рекомендуется выбирать коэффициенты в среднечастотной области ($D_i[3, 4]$ и $D_i[4, 3]$, $D_i[3, 5]$ и $D_i[5, 3]$, $D_i[4, 5]$ и $D_i[5, 4]$).
5. Если встраиваемый бит равен 0, то разность модулей пары коэффициентов дискретного косинусного преобразования должна превышать пороговое значение M_0 , для встраивания единичного бита разность должна быть меньше M_0 . Поэтому для встраивания нулевого бита увеличивается модуль первого коэффициента и на ту же величину уменьшается модуль второго. Для встраивания единичного бита наоборот уменьшается модуль первого коэффициента и на ту же величину увеличивается модуль второго коэффициента.
6. Выполняются пункты 4 и 5 для каждого блока.
7. Выполнить обратное дискретное косинусное преобразование для каждого блока.

Изменение среднечастотных компонент дискретного косинусного преобразования позволяет минимизировать визуальные эффекты встраивания. Встраивание в низкочастотные компоненты приводит к заметному изменению фона изображения. Встраивание в высокочастотные компоненты приводит к потере мелких деталей изображения.

При извлечении встроенного сообщения считается, что известны пары изменяемых коэффициентов дискретного косинусного преобразования. Первые четыре пункта алгоритма извлечения совпадают с пунктами алгоритма встраивания. Остальные шаги алгоритма имеют вид:

5. Найти модуль разности модулей пар коэффициентов дискретного косинусного преобразования, в которое осуществлялось встраивание.
6. Если разность превышает M_0 , то был встроен нулевой бит, в противном случае – единичный.
7. Последовательно определяем встроенные биты для каждого блока.

Для атаки на алгоритм Коха-Жао необходимо определить используемые пары коэффициентов дискретного косинусного преобразования и пороговое значение M_0 . При осуществлении стегоанализа будем исходить из трех предположений:

1. Встраивание происходит в непрерывную область, то есть используются подряд идущие блоки.
2. Во всех блоках для встраивания используется одни и те же пары коэффициентов.
3. Во всех блоках используется одно и то же пороговое значение.

2 Стеганографический анализ

Для решения задач стегоанализа будем исходить из того, что пороговое значение M_0 должно иметь большое значение. В противном случае особенности изображения, используемого в качестве контейнера, могут приводить к ошибкам при извлечении данных.

На первом этапе необходимо выявить пары коэффициентов дискретного косинусного преобразования, используемые для встраивания информации. По аналогии с алгоритмом извлечения сообщения разобьем изображение-контейнер на блоки B_i ($i = 1, \dots, N$) размером 8×8 пикселей. Выполним дискретное косинусное преобразование для каждого блока B_i ($i = 1, \dots, N$) и найдем матрицы коэффициентов D_i ($i = 1, \dots, N$), которые также имеют размер 8×8 . Выполним анализ элементов матриц D_i ($i = 1, \dots, N$). Для этого построим три последовательности:

$$\begin{aligned} C_i(1) &= ||D_i[3, 4]| - |D_i[4, 3]|, \quad i = 1, \dots, N, \\ C_i(2) &= ||D_i[3, 5]| - |D_i[5, 3]|, \quad i = 1, \dots, N, \\ C_i(3) &= ||D_i[4, 5]| - |D_i[5, 4]|, \quad i = 1, \dots, N. \end{aligned}$$

Если встраивание было осуществлено в среднечастотную компоненту, то одна из этих последовательностей должна значительно измениться. Для каждой из последовательностей $C_i(j)$ ($j = 1, 2, 3$; $i = 1, \dots, N$) проанализируем гистограмму зависимости от номера блока i . Встроенное сообщение приводит к появлению

измененного блока в виде ступенчатой зависимости. Причем высота ступени зависит от порогового значения M_0 . Примеры гистограмм для последовательности без встроенного сообщения приведен на рисунке 1, а аналогичная последовательность с встроенным сообщением на рисунке 2.

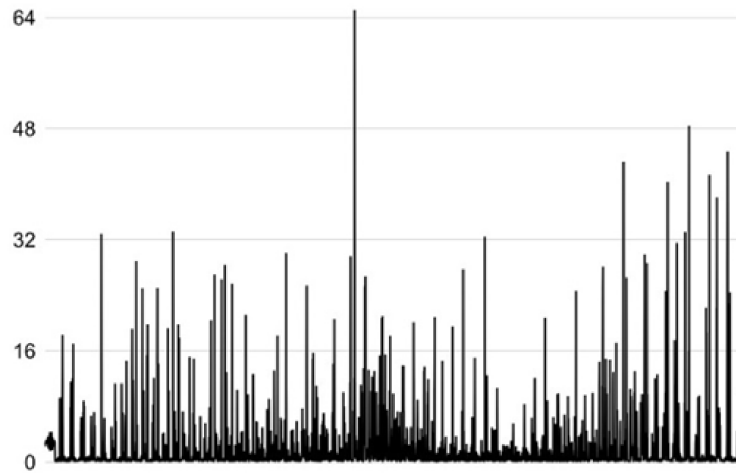


Рис. 1: Гистограмма зависимости $C_i(1)$ без встроенного сообщения.

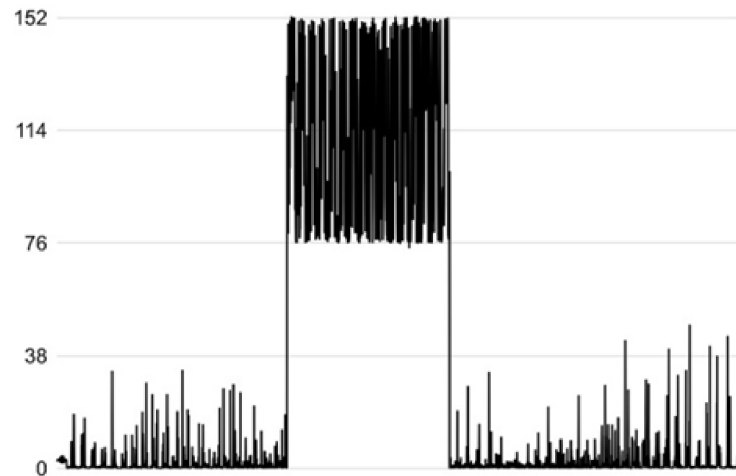


Рис. 2: Гистограмма зависимости $C_i(1)$ с встроенным сообщением.

Таким образом стегоанализ алгоритма Коха-Жао сводится к анализу зависимости последовательностей $C_i(j)$ ($j = 1, 2, 3; i = 1, \dots, N$) и выявлению участка ступенчатых изменений. После обнаружения ступенчатых участков необходимо определить их границы. Для этого выполним численное дифференцирование зависимости $C_i(j)$ ($j = 1, 2, 3; i = 1, \dots, N$) по i с использованием конечных разностей.

$$dC_i(j) = C_i(j) - C_{i-1}(j).$$

В точках ступенчатого изменения после дифференцирования будут наблюдаться высокие пики, соответствующие границе встраивания сообщения. Гистограмма $dC_i(j)$ для случая встроенного представлена на рисунке 3.

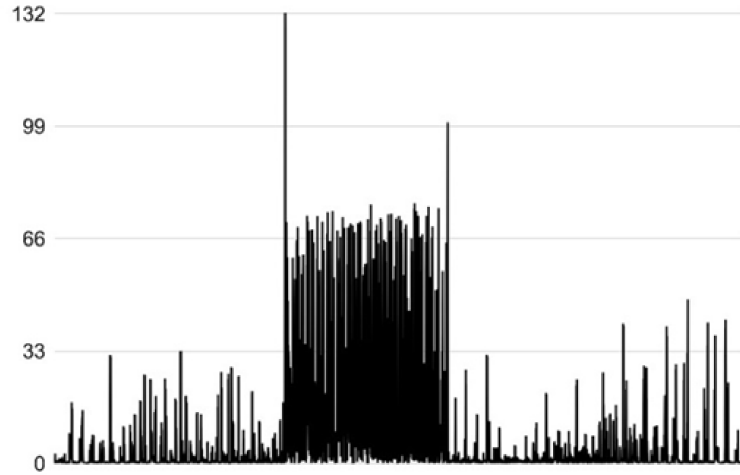


Рис. 3: Гистограмма последовательности $d_i(1)$ с встроенным сообщением.

Поставим задачу автоматического определения границ области встраивания. Для этого для каждой последовательности $d(j)$ определим несколько характеристик: M_j – максимальное значение элементов последовательности $d(j)$, N_j – среднее значение элементов последовательности $d(j)$, O_j – среднеквадратичное отклонение для элементов последовательности $d(j)$. Далее вычислим $R_j = N_j + O_j$. Введем переменную Y_j , принадлежащую интервалу $[R_j, M_j]$. Подберем такое значение Y_j , чтобы существовало ровно два элемента последовательности $d(j)$, превышающих его: $C_{i1}(j) > Y_j$ и $C_{i2}(j) > Y_j$. Полученные индексы элементов i_1 и i_2 являются границами встраивания сообщения. Для определения порогового значения M_0 найдем значение минимального элемента последовательности $C_i(j)$ на интервале $[i_1, i_2]$.

Алгоритм выявления встроенного изображения принимает вид:

1. Разбить изображение на блоки B_i размером 8×8 пикселей.
2. К каждому блоку B_i применить дискретное косинусное преобразование и получить матрицы коэффициентов дискретного косинусного преобразования D_i .
3. Вычислить элементы трех последовательностей величин:

$$C_i(1) = ||D_i[3, 4]| - |D_i[4, 3]||, \quad i = 1, \dots, N,$$

$$C_i(2) = ||D_i[3, 5]| - |D_i[5, 3]||, \quad i = 1, \dots, N,$$

$$C_i(3) = ||D_i[4, 5]| - |D_i[5, 4]||, \quad i = 1, \dots, N.$$

4. Выполнить численное дифференцирование каждой из последовательностей $C_i(j)$ по i :

$$dC_i(j) = C_i(j) - C_{i-1}(j) \quad j = 1, 2, 3 \quad i = 1, \dots, N.$$

5. Вычислить: M_j - максимальное значение элементов массива $d(j)$, N_j - среднее значение элементов массива $d(j)$, O_j - среднеквадратичное отклонение для элементов массива $d(j)$, $R_j = N_j + O_j$.

6. Перебрать различные значения величины Y_j в интервале от R_j до M_j с шагом dY . Определить Y_j такое, что существует ровно два значения $C_{i1}(j) > Y_j$ и $C_{i2}(j) > Y_j$. Если такое значения определить невозможно, то уменьшить шаг dY . Определить i_1 и i_2 .

7. Найти минимальное значение $C_i(j)$ на интервале от i_1 до i_2 . Присвоить M_0 найденное значение.

8. Извлечь сообщение, используя найденные параметры.

Компьютерный эксперимент показал, что данный алгоритм позволяет безошибочно находить и извлекать встроенное сообщение при значениях $M_0 > 54$.

Заключение

Стегоанализ алгоритма стеганографического встраивания Коха-Жао, проведенный в данной статье, выявил неустойчивость к атаке анализа коэффициентов дискретного косинусного преобразования. Предло-

женный в статье алгоритм позволяет с высокой точностью определить положение встроенного сообщения и извлечь его. Алгоритм применим при встраивании в непрерывную область.

Список литературы

- [1] D. Comer. The ubiquitous b-tree. *Computing Surveys*, 11(2):121–137, June 1979.
- [2] D.E. Knuth. *The Art of Computer Programming – Volume 3 / Sorting and Searching*. Addison-Wesley, 1973.
- [3] URL: <http://www.ict.edu.ru/ft/004793/Crypto-1.pdf>.
- [4] N. Provos, P. Honeyman. Detecting steganographic content on the internet. *Technical Report CITI 01-1a* University of Michigan, 2001.
- [5] A. Westfeld, A. Pfitzmann. Attacks on Steganographic Systems: Breaking the Steganographic Utilities EzStego, Jsteg, Steganos and STools- and Some Lessons Learned. *3rd International Workshop on Information Hiding*, 2000.
- [6] D.E. Vilkhovskiy, S.V. Belim. Detection the Stego-Insertions Like LSB-Substitution in Bitmap Images. *CEUR Workshop Proceedings*, 1965, 2017. URL: <http://ceur-ws.org/Vol-1965/paper11.pdf>
- [7] S.V. Belim, D.E. Vilkhovskiy. Usage of analytic hierarchy process for steganographic inserts detection in images. *2016 Dynamics of Systems, Mechanisms and Machines (Dynamics)*:1–5, 2016. URL: <http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7818977&isnumber=7818960>
- [8] S.V. Belim, D.E. Vilkhovskiy. Steganalysis Algorithm Based on Heirarchy Analysis Method. *CEUR Workshop Proceedings*, 1732, 2016. URL: <http://ceur-ws.org/Vol-1732/paper7.pdf>.
- [9] S.V. Belim, D.E. Vilkhovskiy. Algorithm for detection of steganographic inserts type LSB-substitution on the basis of an analysis of the zero layer. *Journal of Physics: Conf. Series*, 944:012012(1–6), 2017.
- [10] E. Koch, J. Zhao. Towards robust and hidden image copyright labeling. *IEEE Workshop on Nonlinear Signal and Image Processing*:452–455, 1995.

Steganographic Analysis of the Koch-Zhao Algorithm

Sergey V. Belim, Danil E. Vilkhovskiy

The analysis of a steganographic Koch-Zhao algorithm is carried out. The possibility the attack to detection of the message is considered. The algorithm for calculation of message limits is suggested. The computer experiment is made. The inserting parameters, allowing to carry out the attack, are determined.